FINITE SEMIFIELDS AND NONSINGULAR TENSORS

MICHEL LAVRAUW

Abstract. In this article, we give an overview of the classification results in the theory of finite semifields[1]and elaborate on the approach using nonsingular tensors based on Liebler [52].

1. Introduction and classification results of finite semifields

1.1. **Definition, examples and first classification results.**

Finite semifields are a generalisation of finite fields (where associativity of multiplication is not assumed) and the study of finite semifields originated as a classical part of algebra in the work of L. E. Dickson and A. A. Albert at the start of the 20th century.

Remark 1.1. *The name semifield was introduced by Knuth in his dissertation (*[41]*). In the literature before that, the algebraic structure, satisfying (S1)-(S4), was called a distributive quasifield, a division ring or a division algebra. Since the 1970's the use of the name semifields has become the standard.*

Due to the Dickson-Wedderburn Theorem which says that each finite skew field is a field (see [36, Section 2] for some historical remarks), finite semifields are in some sense the algebraic structures closest to finite fields. It is therefore not surprising that Dickson took up the study of finite semifields shortly after the classification of finite fields at the end of the 19th century (announced by E. H. Moore on the International Congress for Mathematicians in Chicago in 1893).

Remark 1.2. *In the remainder of this paper we only consider finite semifields (unless stated otherwise) and finiteness will often be assumed implicitly. In the infinite case, the octonions (see e.g.* [8] *for a very interesting account on them) are an example of a proper semifield. They can be constructed in various ways, for example as a Cayley-Dickson algebra from the quaternions.*

For future reference, we continue with a formal definition of a semifield. A *finite semifield* $(\mathbb{S}, +, \circ)$ is an algebra of finite dimension over a finite field $\mathbb{F}$ with at least two elements, and two binary operations $+$ and $\circ$, satisfying the following axioms.

(S1) $(\mathbb{S}, +)$ is a group with identity element 0.
(S2) $x \circ (y + z) = x \circ y + x \circ z$ and $(x + y) \circ z = x \circ z + y \circ z$, for all $x, y, z \in \mathbb{S}$.
(S3) $x \circ y = 0$ implies $x = 0$ or $y = 0$.

[1] Note that this is not intended as a survey of finite semifields including a complete state of the art (see also Remark 1.10).

The author acknowledges the support of the Fund for Scientific Research - Flanders (FWO)
(Email: michel.lavrauw@unipd.it).

(S4) $\exists 1 \in \mathbb{S}$ such that $1 \circ x = x \circ 1 = x$, for all $x \in \mathbb{S}$.

We call a semifield *non-trivial* or *proper* if it is not associative. One easily shows that the additive group of a finite semifield is elementary abelian. Rewriting the expression $(a+b)\circ(c+d)$ in two ways using (S1) and (S2), we get $a\circ d + b\circ c = b\circ c + a\circ d$. Since any two elements $x, y \in \mathbb{S}$ can be written as a product $x = a\circ d$ and $y = b\circ c$ for some $a, b, c, d \in \mathbb{S}$, the additive group is abelian. By way of contradiction one also shows that the additive order of each nonzero element is a prime number p, and the additive group is elementary abelian. The additive order of the elements of $\mathbb{S}$ is called the *characteristic* of $\mathbb{S}$.

Relying on this property we will often denote a semifield by $(\mathbb{S}, \circ)$ instead of $(\mathbb{S}, +, \circ)$.

Example 1.3. *The first non-trivial examples of semifields (i.e. not fields) were constructed by Dickson in* [23], [24] *and can be described as follows: a semifield* $(\mathbb{F}_{q^k}^2, +, \circ)$ *of order* q^{2k} *with addition and multiplication defined by*

$$\begin{cases} (x,y)+(u,v) & = (x+u, y+v) \\ (x,y)\circ(u,v) & = (xu+\alpha y^q v^q, xv+yu) \end{cases} \tag{1}$$

where q *is an odd prime power and* α *is a non-square in* $\mathbb{F}_{q^k}$*. Note that* $\mathbb{S}$ *is commutative but not associative. The identity element is* $(1,0)$*.*

These first examples were crucial in the light of the above mentioned Dickson-Wedderburn theorem. Also the first classification result (also valid in the infinite case) was readily proved by Dickson in [23].

Theorem 1.4 ([23]). *A two-dimensional (infinite or finite) semifield is a field.*

Proof. Consider a basis $\{1, x\}$ for $\mathbb{S}$ over the field K. Multiplication in $\mathbb{S}$ is defined by $x\circ x = ax+b$, $a, b \in K$. If x^2-ax-b is not irreducible in $K[x]$, then there exist $x_1, x_2 \in K$ such that $(x-x_1)\circ(x-x_2) = 0$, a contradiction. It follows that $\mathbb{S} = K(x)$. □

An algebra satisfying all of the axioms of a semifield except (S4) is called a *pre-semifield.* By what is sometimes called Kaplansky's trick ([39, page 957]), a semifield with identity $u\circ u$ is obtained from a pre-semifield by defining a new multiplication $\hat{\circ}$ as follows

$$(x\circ u)\hat{\circ}(u\circ y) = x\circ y. \tag{2}$$

Example 1.5. *An important example of pre-semifields are the so-called generalised twisted fields (or (Albert) twisted fields) constructed by A. A. Albert in* [4]*, where multiplication on* $\mathbb{F}_{q^n}$ *is defined by*

$$x\circ y = xy - \eta x^\alpha y^\beta,$$

$\alpha, \beta \in Aut(\mathbb{F}_{q^n})$*,* $Fix(\alpha) = Fix(\beta) = \mathbb{F}_q$*, where* $\eta \in \mathbb{F}_{q^n} \setminus \{x^{\alpha-1}y^{\beta-1} : x, y \in \mathbb{F}_{q^n}\}$*. This defines a proper pre-semifield if* $\alpha \neq \beta$*,* $\alpha \neq 1$ *and* $\beta \neq 1$*. In order to obtain a semifield with unit* $1\circ 1 = 1-\eta$*, we define a new multiplication:*

$$(x-\eta x^\alpha)\hat{\circ}(y-\eta y^\beta) = xy - \eta x^\alpha y^\beta.$$

As one can imagine from this example, the formula for the multiplication of a semifield can be more complicated than for the pre-semifield, and therefore it is sometimes more convenient to work with pre-semifields instead of semifields. We will come back to this issue in Remark 1.6.

The importance of generalised twisted fields is illustrated by the following classification result of Menichetti published in 1977. In order to state the result we need to introduce the concept of isotopism (introduced by Albert in 1942 [1, page 696]); a notion that might seem artificial at first but will become relevant in view of the connection between semifields and projective planes.

An *isotopism* (or *isotopy*) between two (pre-)semifields $(\mathbb{S}, \circ)$ and $(\mathbb{S}', \circ')$ is a triple (F, G, H) of nonsingular linear maps from $\mathbb{S}$ to $\mathbb{S}'$ such that

$$x^F \circ' y^G = (x \circ y)^H,$$

for all $x, y \in \mathbb{S}$. If such an isotopism exists, the (pre-)semifields $\mathbb{S}$ and $\mathbb{S}'$ are called *isotopic* and the isotopism class of a (pre-)semifield $\mathbb{S}$ is denoted by $[\mathbb{S}]$. If H is the identity, the isotopism is called *principal.* If $F = G$, then $\mathbb{S}$ and $\mathbb{S}'$ are called *strongly isotopic.*

Remark 1.6. *Note that Kaplansky's trick illustrates that each pre-semifield $\mathbb{S}$ is isotopic to a semifield; an isotopism is given by (R_u, L_u, id), where R_u and L_u denote right and left multiplication by u in $(\mathbb{S}, \circ)$. Since in semifield theory one is mainly concerned with the isotopism classes of semifields, this justifies working with pre-semifields instead of semifields when convenient. (For instance if we don't find an easy enough formula for the semifield multiplication.)*

Now we can state the classification conjectured by Kaplansky and proved by Menichetti in 1977.

Theorem 1.7 ([58]). *A three-dimensional finite semifield is a field or is isotopic to a generalised twisted field.*

About twenty years later, Menichetti generalised his result to the following.

Theorem 1.8 ([59]). *Let $\mathbb{S}$ be a semifield of prime dimension n over $\mathbb{F}_q$. Then there exists an integer $\nu(n)$ depending only on n, such that if $q > \nu(n)$ then $\mathbb{S}$ is isotopic to a generalised twisted field.*

Apart from classification results for small orders, these are the only classification results of finite semifields without extra hypotheses on the nuclei (defined below).

Concerning the existence of proper semifields, we have the following theorem (see e. g. [41, Theorem 6.1 and Corollary 8.2.2]).

Theorem 1.9. *A proper semifield of order p^n exists iff and only if $n \geq 3$ and $p^n \geq 16$.*

This means that the smallest non-associative semifield has order 16. Exhaustive computer searches have led to the classification of semifields of order 16 in [40], 32 in [71], 64 in [65], 81 in [21], 256 (with center $\mathbb{F}_4$) and 625 in [66]. It should be noted that although numerous constructions and examples were obtained before 2009, most of the semifields of order 64 found by computer in [65] were new. In total 80 Knuth orbits (see below for a definition) were found, and only 13 were previously known.

Remark 1.10. *There are many interesting questions concerning finite semifields that we will not address in this article. For instance, we will not give an overview of all the known constructions of semifields. There are too many constructions by now and sometimes the* *isotopism classes overlap or even generalize previous construction. A reasonably updated list can be found in* [48]*, although not complete since new constructions have been obtained since the writing of* [48]*. Many examples of commutative semifields have recently been constructed (in part motivated by the links with perfect nonlinear functions) see e.g.* [18]*,* [10]*,* [15]*. For isotopism relations between the recent constructions we refer to* [56]*, and to* [64] *for an approach to planar functions using character theory. For a discussion on the number of isotopism classes of semifields of given order, see* [36]*. The number of isotopism classes of cyclic semifields has been investigated in* [38]*,* [22] *and* [49]*. The existence of a primitive element for the multiplicative group of a semifield has been investigated in* [67] *and* [26]*. For more on the autotopism group of semifields and its solubility we refer to* [30]*,* [51]*, and for a more general account on the isotopism groups of ternary rings we refer to* [6]*. For more on the multiplication group of semifields we refer to* [60] *and for a study of the automorphisms of p-groups of semifield type, see* [27]*. The existence of subplanes of order q^k in some semifield planes of order q^n where k does not divide n, has been established in* [67] *and further investigated in* [31] *and* [63]*.*

1.2. **The nuclei of a semifield.** The nuclei of a semifield arise in a similar way as the (commutative) center of non-commutative algebraic structures. However, while the commutative center is uniquely defined for a non-commutative structure, there are four different associative substructures to consider for non-associative structures. These are called the nucleus, the left nucleus, the middle nucleus, and the right nucleus and are defined as follows.

The subset

$$\mathbb{N}_l(\mathbb{S}) := \{x \ : \ x \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall y, z \in \mathbb{S}\},$$

is called the *left nucleus* of $\mathbb{S}$. Analogously, one defines the *middle nucleus*

$$\mathbb{N}_m(\mathbb{S}) := \{y \ : \ y \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, z \in \mathbb{S}\},$$

and the *right nucleus*

$$\mathbb{N}_r(\mathbb{S}) := \{z \ : \ z \in \mathbb{S} \mid x \circ (y \circ z) = (x \circ y) \circ z, \ \forall x, y \in \mathbb{S}\}.$$

The intersection of these three nuclei is called the *nucleus* or *associative center* $\mathbb{N}(\mathbb{S})$, while the intersection of the associative center and the *commutative center* $C(\mathbb{S})$ (defined in the usual way) is called the *center* of $\mathbb{S}$ and denoted by $Z(\mathbb{S})$. One easily verifies that all of these substructures are finite fields and $\mathbb{S}$ can be seen as a (left or right) vectorspace over these substructures. Indeed, apart from the usual representation of a semifield as a finite-dimensional algebra over its center, a semifield can also be viewed as a left vector space $V_l(\mathbb{S})$ over its left nucleus; as a left vector space $V_{lm}(\mathbb{S})$ and right vector space $V_{rm}(\mathbb{S})$ over its middle nucleus; as a right vector space $V_r(\mathbb{S})$ over its right nucleus; and as a left or right vector space over its nucleus (the latter is rarely considered). Left (resp. right) multiplication in $\mathbb{S}$ by an element x is denoted by L_x (resp. R_x), i.e. $y^{L_x} = x \circ y$ (resp. $y^{R_x} = y \circ x$). It follows that L_x is an endomorphism of $V_r(\mathbb{S})$, while R_x is an endomorphism of $V_l(\mathbb{S})$.

Remark 1.11. *Although each pre-semifield is isotopic to a semifield, it is important to note that we have only defined the nuclei for semifields, and not for pre-semifields. This is because of the following. Suppose we define the nucleus for a pre-semifield in the same way as for a semifield $\mathbb{S}$. Using the same notation as above we get the following.*

(a) *If* $(\mathbb{S}, +, \circ)$ *is a finite pre-semifield, then the following three statements are equivalent:*
   (i) $(\mathbb{S}, +, \circ)$ *is a semifield,*
   (ii) $\mathbb{N}_m(\mathbb{S}) \neq \{0\}$,
   (iii) $\mathbb{N}_l(\mathbb{S}) \neq \{0\}$ *and* $\mathbb{N}_r(\mathbb{S}) \neq \{0\}$.

Proof. (i)⇒ (ii), (iii) If $(\mathbb{S}, +, \circ)$ is a semifield, and e is the identity element of $(\mathbb{S}, \circ)$, then it is straigtforward to show that e belongs to all three of the nuclei $\mathbb{N}_l(\mathbb{S})$, $\mathbb{N}_m(\mathbb{S})$, and $\mathbb{N}_r(\mathbb{S})$. Hence (i) implies (ii) and (iii).
(ii) ⇒ (i) Let $a \in \mathbb{N}_m(\mathbb{S}) \neq \{0\}$. Then one easily verifies that $\mathbb{N}_m(\mathbb{S})$ is a finite field. Suppose e_m is the identity element of $(\mathbb{N}_m(\mathbb{S}), \circ)$. Then

$$e_m \circ (a \circ x) = (e_m \circ a) \circ x = a \circ x, \ \forall x \in \mathbb{S},$$

and

$$(y \circ a) \circ e_m = y \circ (a \circ e_m) = y \circ a, \ \forall y \in \mathbb{S}.$$

Since every element $z \in \mathbb{S}$ can be written as $z = a \circ x = y \circ a$ for some $x, y \in \mathbb{S}$, this implies that e_m is the identity element for $(\mathbb{S}, \circ)$. Hence (i) follows from (ii).
(iii) ⇒ (i) Let $a \in \mathbb{N}_l(\mathbb{S}) \neq \{0\}$. Again one easily verifies that $\mathbb{N}_l(\mathbb{S})$ is a finite field. Suppose e_l is the identity element of $(\mathbb{N}_l(\mathbb{S}), \circ)$. Then

$$e_l \circ (a \circ x) = (e_l \circ a) \circ x = a \circ x, \ \forall x \in \mathbb{S}.$$

Since every element of $\mathbb{S}$ can be written as $a \circ x$ for some $x \in \mathbb{S}$, we have that $e_l \circ x = x$, $\forall x \in \mathbb{S}$. Similarly it follows that $x \circ e_r = x$, $\forall x \in \mathbb{S}$ where e_r is identity of $(\mathbb{N}_r(\mathbb{S}), \circ)$. But then $e_l = e_l \circ e_r = e_r$, which implies that e_l is the identity element for $(\mathbb{S}, \circ)$. This shows that also (iii) implies (i). □

In [20, page 237]*, the nuclei are defined for pre-semifields. On page 238, the author states that all three of the nuclei* $\mathbb{N}_l(\mathbb{S})$*,* $\mathbb{N}_m(\mathbb{S})$*, and* $\mathbb{N}_r(\mathbb{S})$ *are Galois fields, and that* $\mathbb{N}_l(\mathbb{S}) \cap Z_c(\mathbb{S})$*,* $\mathbb{N}_m(\mathbb{S}) \cap Z_c(\mathbb{S})$*, and* $\mathbb{N}_r(\mathbb{S}) \cap Z_c(\mathbb{S})$*, where* $Z_c(\mathbb{S})$ *is the commutative centre of* $\mathbb{S}$*, are Galois fields of the same characteristic as* $\mathbb{S}$*. The above shows that this is incorrect. We have an immediate corollary.*

(b) *If* $(\mathbb{S}, +, \circ)$ *is a pre-semifield but not a semifield, then* $\mathbb{N}_m(\mathbb{S}) = \{0\}$.

However if $(\mathbb{S}, +, \circ)$ *is a semifield, then we do have the following.*

(c) *If* $(\mathbb{S}, +, \circ)$ *is a semifield, then the nuclei are finite fields containing the prime field of* $\mathbb{S}$.

Nevertheless, there is a way to define certain fields K_l*,* K_m *and* K_r *related to a pre-semifield* $\mathbb{S}$ *such that they are equal (as finite fields) to the nuclei of any semifield isotopic to* $\mathbb{S}$ *(see* [56]*). The definition of these fields uses the endomorphisms of left and right multiplication as follows. As we mentioned before* L_x *is an endomorphism of* $V_r(\mathbb{S})$*, while* R_y *is an endomorphism of* $V_l(\mathbb{S})$*. But if we consider* L_x *and* R_y *as elements of* $\mathrm{End}(\mathbb{S})$*, and we denote the set of all* L_x *by* $\mathcal{L}$ *and all* R_y *by* $\mathcal{R}$*, then define* K_l *(resp.* K_r*) as the largest field in* $\mathrm{End}(\mathbb{S})$ *such that* $\mathcal{L}K_l \subset \mathcal{L}$ *(resp.* $\mathcal{R}K_r \subset \mathcal{R}$*). The field* K_m *is defined as the largest subfield of* $\mathrm{End}(\mathbb{S})$ *such that* $K_m\mathcal{R} \subset \mathcal{R}$ *(or equivalently* $K_m\mathcal{L} \subset \mathcal{L}$*). These subfields of* $\mathrm{End}(\mathbb{S})$ *correspond to the nuclei of a semifield isotopic to* $\mathbb{S}$ *(and hence of all* *semifields isotopic to $\mathbb{S}$). If the nuclei of a pre-semifield would be defined like this, then the above statement from* [20] *holds true.*

1.3. **Classification results.** Before we continue with classification results depending on the size of the nuclei, we mention some of the earlier purely algebraic characterisations of finite fields. Some of these characterisations use the notion of associator. As the commutator ($[x, y] = x \circ y - y \circ x$) is a test for commutativity, the *associator*, defined as

$$[a, b, c] := (a \circ b) \circ c - a \circ (b \circ c),$$

is a test for associativity. Different types of identities involving the commutator and associator lead to various sorts of algebras studied in the literature. Of relevance in the theory of semifields is the following. If $[a, a, b] = [a, b, a] = [b, a, a] = 0$, for all $a, b \in \mathbb{S}$, then $\mathbb{S}$ is called *alternative*. The term "alternative" is motivated by the fact that this property implies that the associator is alternating, i.e. changes sign whenever two of the arguments are interchanged. It also implies that each subalgebra generated by two elements is associative. This leads up to the Artin-Zorn Theorem (see [72]).

Theorem 1.12. *Every finite alternative semifield is a field.*

Remark 1.13. *The Artin-Zorn Theorem is the finite version of the Bruck-Kleinfeld-Skornyakov Theorem (*[14], [68]*), which says that an alternative semifield is associative or a Cayley-Dickson algebra over its center.*

Albert generalised the concept of alternative algebras to *power-associative* algebras, which satify the property $[a^i, a^j, a^k] = 0$, for all $a \in \mathbb{S}$, $i, j, k \in \mathbb{N}$. This property implies that each subalgebra generated by one element is associative. In [2] Albert gives the following nice characterisation of finite fields.

Theorem 1.14. *Every finite power-associative semifield of characteristic $p \neq 2$ whose center has more than five elements is a finite field.*

All the other classification results for semifields of given order involve conditions on one or more of their nuclei. In fact, all of them deal with rank two semifields (two-dimensional over one of their nuclei).

The first result in this direction is the following theorem that can be found in [29] (case (a)) and in [42, Theorem 7.4.1].

Theorem 1.15. *Let $\mathbb{S}$ be a semifield which is not a field and which is a 2-dimensional vector space over a finite field $\mathbb{F}$. Then*

(1) $\mathbb{F} = \mathbb{N}_r = \mathbb{N}_m$ *if and only if* $\mathbb{S}$ *is a Knuth semifield of type II.*
(2) $\mathbb{F} = \mathbb{N}_l = \mathbb{N}_m$ *if and only if* $\mathbb{S}$ *is a Knuth semifield of type III.*
(3) $\mathbb{F} = \mathbb{N}_l = \mathbb{N}_r$ *if and only if* $\mathbb{S}$ *is a Knuth semifield of type IV.*

Another strong result was obtained by Cohen and Ganley in 1982 [17], concerning commutative semifields that are two-dimensional over their middle nucleus. We say that a semifield $\mathbb{S}$ is a *rank two commutative semifield* (RTCS), if $\mathbb{S}$ is commutative and of dimension at most two over its middle nucleus.

Rewriting the example (1) from Dickson, we have the following construction of an RTCS. Let σ be an automorphism of $\mathbb{F}_q$, q odd, and define the following multiplication on $\mathbb{F}_q^2$:

$$(x, y) \circ (u, v) = (xv + yu, yv + mx^\sigma u^\sigma), \tag{3}$$

where m is a non-square in $\mathbb{F}_q$. Cohen and Ganley made significant progress in the investigation of RTCS. They put Dickson's construction in the following more general setting. Let $\mathbb{S}$ be an RTCS of order q^2 with middle nucleus $\mathbb{F}_q$, and let $\alpha \in \mathbb{S} \setminus \mathbb{F}_q$ be such that $\{1, \alpha\}$ is a basis for $\mathbb{S}$. Addition in $\mathbb{S}$ is component-wise and multiplication is defined as

$$(x, y) \circ (u, v) = (xv + yu + g(xu), yv + f(xu)), \tag{4}$$

where f and g are additive functions from $\mathbb{F}_q$ to $\mathbb{F}_q$, such that $x\alpha^2 = g(x)\alpha + f(x)$. We denote this semifield by $\mathbb{S}(f, g)$. Verifying that this multiplication has no zero divisors leads to the following theorem which comes from [17].

Theorem 1.16. *Let $\mathbb{S}$ be a RTCS of order q^2 and characteristic p. Then there exist $\mathbb{F}_p$-linear functions f and g such that $\mathbb{S} = \mathbb{S}(f, g)$, with multiplication as in (4) and such that $zw^2 + g(z)w - f(z) = 0$ has no solutions for all w, $z \in \mathbb{F}_q$, and $z \neq 0$.*

For q even, Cohen and Ganley obtained the following remarkable theorem proving the non-existence of proper RTCS in even characteristic.

Theorem 1.17 ([17]). *For q even the only RTCS of order q^2 is the finite field $\mathbb{F}_{q^2}$.*

If q is odd, then the quadratic $zw^2 + g(z)w - f(z) = 0$ in w will have no solutions in $\mathbb{F}_q$ if and only if $g(z)^2 + 4zf(z)$ is a non-square for all $z \in \mathbb{F}_q^*$. In [17], Cohen and Ganley prove that in odd characteristic, in addition to the example with multiplication (3) by Dickson, there is just one other infinite family of proper RTCS, namely of order 3^{2r}, with multiplication given by:

$$(x, y) \circ (u, v) = (xv + yu + x^3u^3, yv + \eta x^9u^9 + \eta^{-1}xu), \tag{5}$$

with η a non-square in $\mathbb{F}_{3^r}$ $(r \geq 2)$.

Theorem 1.18 ([17][1]). *Suppose that f and g are linear polynomials of degree less than q over $\mathbb{F}_q$, q odd, such that for infinitely many extensions $\mathbb{F}_{q^e}$ of $\mathbb{F}_q$, the functions*

$$f^* : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e} \ : \ x \mapsto f(x), \text{ and}$$
$$g^* : \mathbb{F}_{q^e} \to \mathbb{F}_{q^e} \ : \ x \mapsto g(x),$$

define an RTCS $\mathbb{S}(f^*, g^*)$ of order q^{2e}. Then $\mathbb{S}(f, g)$ is a semifield with multiplication given by (3) or (5), or $\mathbb{S}(f, g)$ is a field.

The only other example of an RTCS was constructed from a translation ovoid of $Q(4, 3^5)$, first found by computer in 1999 by Penttila and Williams ([61]). The associated semifield has order 3^{10} and multiplication

$$(x, y) \circ (u, v) = (xv + yu + x^{27}u^{27}, yv + x^9u^9). \tag{6}$$

Summarising, the only known examples of RTCS which are not fields are of *Dickson type* (3), of *Cohen-Ganley type* (5), or of *Penttila-Williams type* (6).

[1] See also Theorem 1(a) of [7], where the proof does not involve arguments about infinite families (see bottom of page 411 in [7]).

The existence of RTCS was further examined[2] in [12] and [45] obtaining the following theorems which show that there is little room for further examples.

Theorem 1.19 ([45]). *Let $\mathbb{S}$ be an RTCS of order p^{2n}, p an odd prime. If $p > 2n^2 - (4 - 2\sqrt{3})n + (3 - 2\sqrt{3})$, then $\mathbb{S}$ is either a field or a RTCS of Dickson type.*

Theorem 1.20 ([12]). *Let $\mathbb{S}$ be an RTCS of order q^{2n}, q an odd prime power, with center $\mathbb{F}_q$. If $q \geq 4n^2 - 8n + 2$, then $\mathbb{S}$ is either a field or a RTCS of Dickson type.*

In combination with a computational result by Bloemen, Thas, and Van Maldeghem [11], the above implies a complete classification of RTCS of order q^6, with centre of order q.

Theorem 1.21 ([12]). *Let $\mathbb{S}$ be an RTCS of order q^6 with centre of order q, then either $\mathbb{S}$ is a field, or q is odd and $\mathbb{S}$ is of Dickson type.*

More recently, using the geometric approach using the linear sets the following results for rank two semifields of order q^4 and q^6 have been obtained in [16] and [34], respectively.

Theorem 1.22 ([16]). *A semifield $\mathbb{S}$ of order q^4 with left nucleus $\mathbb{F}_{q^2}$ and center $\mathbb{F}_q$ is isotopic to one of the following semifields: Generalized Dickson/Knuth semifields (q odd), Hughes-Kleinfeld semifields, semifields lifted from Desarguesian planes or Generalized twisted fields.*

Theorem 1.23 ([34]). *Each semifield $\mathbb{S}$ of order q^6, with left nucleus of order q^3 and middle and right nuclei of order q^2 and center of order q is isotopic to a JMPT semifield, precisely $\mathbb{S}$ is isotopic to a semifield $(\mathbb{F}_{q^6}, +, \circ)$ with multiplication given by*

$$x \circ y = (\alpha + \beta u)x + b\gamma x^{q^3}, \quad \textit{where} \quad y = \alpha + \beta u + \gamma b \ \ (\alpha, \beta, \gamma \in \mathbb{F}_{q^2}),$$

with u a fixed element of $\mathbb{F}_{q^3} \setminus \mathbb{F}_q$ and b an element of $\mathbb{F}_{q^6}$ such that $b^{q^3+1} = u$.

In [57], [33] and [25], semifields of order q^6, with left nucleus of order q^3 and center of order q, are studied using the same geometric approach, giving the following result.

Theorem 1.24 ([57], [33]). *Let $\mathbb{S}$ be a semifield of order q^6 with left nucleus of order q^3 and center of order q. Then there are eight possible geometric configurations for the corresponding linear set $L(\mathbb{S})$ in $\mathrm{PG}(3, q^3)$. The corresponding classes of semifields are partitioned into eight non-isotopic families.*

2. Semifields and Finite Geometry

As mentioned before, the study of semifields originated around 1900, and the link with projective planes through the coordinatisation method inspired by Hilbert's *Grundlagen der Geometrie* (1999), and generalised by Hall [28] in 1943, was a further stimulation for the development of the theory of finite semifields. Most of what is contained in this section concerning projective planes and the connections with semifields can be found with more details in [20], [30]. For a recent title on the theory of translation planes, see [32]. It is in the context of projective planes that the notion of isotopism is of the essence.

[2] One of the motivations for the study of RTCS arose from the connection with semifield flocks and generalised quadrangles, see e.g. [69], [70].

Starting with a semifield $(\mathbb{S}, \circ)$ one defines an incidence structure $(\mathcal{P}, \mathcal{L}, \mathcal{I})$, where the set of points $\mathcal{P} = \{(0,0,1)\} \cup \{(0,1,c) : c \in \mathbb{S}\} \cup \{(1,a,b) : a,b \in \mathbb{S}\}$ and the set of lines $\mathcal{L} = \{[0,0,1]\} \cup \{[0,1,z] : z \in \mathbb{S}\} \cup \{(1,x,y) : x,y \in \mathbb{S}\}$. The incidence relation $\mathcal{I}$ is defined as follows:

$$(a,b,c)\mathcal{I}[x,y,z] \Leftrightarrow az = b \circ y + cx.$$

If there exists a line ℓ in a projective plane π, such that for each point P on ℓ the group of (P,ℓ)-perspectivities acts transitively on the points of the affine plane $\pi \setminus \ell$, then π is called a *translation plane*, and ℓ is called a translation line of π. If both π and π^d are translation planes, then π is called a *semifield plane.* The point of a semifield plane corresponding to the translation line of the dual plane is called the *shears point.* It can be shown that, unless the plane is Desarguesian, the translation line (shears point) of a translation plane (dual translation plane) is unique, and the shears point of a semifield plane π lies on the translation line of π.

The following diagram inspired by [30] illustrates how semifield planes are related to other types of translation planes. There are six types of planes (eight in the infinite case), and each type is labeled by its name and the associated algebraic structure (in italic).

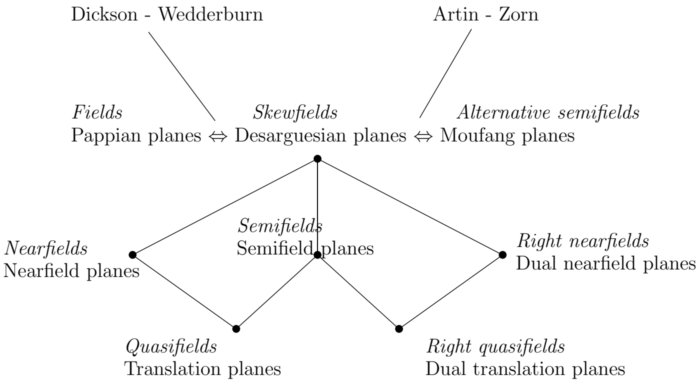

FIGURE 1. Types of finite translation planes and their associated algebraic structures.

The importance of the notion of isotopism arises from the equivalence between the isomorphism classes of projective planes and the isotopism classes of finite semifields, as shown by A. A. Albert in 1960.

THEOREM 2.1 ([3]). *Two semifield planes are isomorphic if and only if the corresponding semifields are isotopic.*

2.1. The Knuth orbit.

If $\mathbb{S}$ is an n-dimensional algebra over the field $\mathbb{F}$, and $\{e_1, \ldots, e_n\}$ is an $\mathbb{F}$-basis for $\mathbb{S}$, then the multiplication can be written in terms of the multiplication of the e_i, i.e., if $x = x_1e_1 + \cdots + x_ne_n$ and $y = y_1e_1 + \cdots + y_ne_n$, with $x_i, y_i \in \mathbb{F}$, then

$$x \circ y = \sum_{i,j=1}^{n} x_iy_j(e_i \circ e_j) = \sum_{i,j=1}^{n} x_iy_j \left(\sum_{k=1}^{n} a_{ijk}e_k\right) \tag{7}$$

for certain $a_{ijk} \in \mathbb{F}$, called the *structure constants* of $\mathbb{S}$ with respect to the basis $\{e_1, \ldots, e_n\}$.

In [42] Knuth noted that the action, of the symmetric group S_3, on the indices of the structure constants gives rise to another five semifields starting from one semifield $\mathbb{S}$. This set of at most six semifields is called the *S_3-orbit* of $\mathbb{S}$, and consists of the semifields $\{\mathbb{S}, \mathbb{S}^{(12)}, \mathbb{S}^{(13)}, \mathbb{S}^{(23)}, \mathbb{S}^{(123)}, \mathbb{S}^{(132)}\}$.

Knuth proved that the action of S_3, defined above, on the indices of the structure constants of a semifield $\mathbb{S}$ is well-defined with respect to the isotopism classes of $\mathbb{S}$, and by the *Knuth orbit of* $\mathbb{S}$ (notation $\mathcal{K}(\mathbb{S})$), we mean the set of isotopism classes corresponding to the S_3-orbit of $\mathbb{S}$, i.e.,

$$\mathcal{K}(\mathbb{S}) = \{[\mathbb{S}], [\mathbb{S}^{(12)}], [\mathbb{S}^{(13)}], [\mathbb{S}^{(23)}], [\mathbb{S}^{(123)}], [\mathbb{S}^{(132)}]\}. \tag{8}$$

The semifield corresponding to the dual plane $\pi(\mathbb{S})^d$ of a semifield plane $\pi(\mathbb{S})$ is the plane $\pi(\mathbb{S}^{opp})$, where $\mathbb{S}^{opp}$ is the *opposite algebra* of $\mathbb{S}$ obtained by reversing the multiplication $\circ$, or in other words, the semifield corresponding to the dual plane is $\mathbb{S}^{(12)}$, which we also denote by $\mathbb{S}^d$, i.e.,

$$\mathbb{S}^d = \mathbb{S}^{(12)} = \mathbb{S}^{opp}. \tag{9}$$

Similarly, it is easy to see that the semifield $\mathbb{S}^{(23)}$ can be obtained by transposing the matrices corresponding to the transformations L_{e_i}, $e_i \in \mathbb{S}$, with respect to some basis $\{e_1, e_2, \ldots, e_n\}$ of $V_r(\mathbb{S})$, and for this reason $\mathbb{S}^{(23)}$ is also denoted by $\mathbb{S}^t$, called the *transpose of* $\mathbb{S}$. With this notation, the Knuth orbit becomes

$$\mathcal{K}(\mathbb{S}) = \{[\mathbb{S}], [\mathbb{S}^d], [\mathbb{S}^t], [\mathbb{S}^{dt}], [\mathbb{S}^{td}], [\mathbb{S}^{dtd}]\}. \tag{10}$$

Taking the transpose of a semifield can also be interpreted geometrically as dualising the semifield spread (Maduram [55]). The resulting action on the set of nuclei of the isotopism class $\mathbb{S}$ is as follows. The permutation (12) fixes the middle nucleus and interchanges the left and right nuclei; the permutation (23) fixes the left nucleus and interchanges the middle and right nuclei. Summarising, the action of the dual and transpose generate a series of at most six isotopism classes of semifields, with nuclei according to Figure 2.

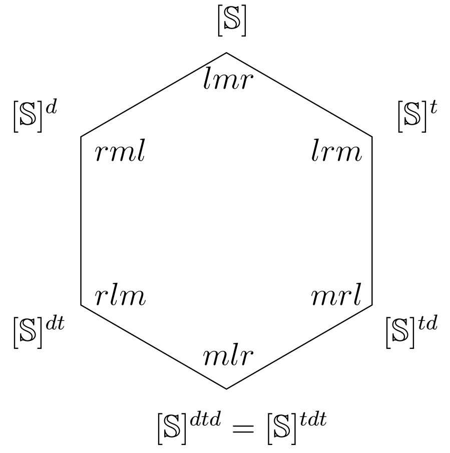

FIGURE 2. The Knuth orbit $\mathcal{K}(\mathbb{S})$ of a semifield $\mathbb{S}$ with nuclei lmr

3. Semifields: a geometric approach

In this section, we explain a geometric approach to finite semifields, which has been very fruitful in recent years. More details of this approach and the links with finite geometry can be found in [48]. This approach naturally breaks up the study of semifields into different parts. First we give a sketch of the general setting, where no assumptions on the nuclei or other properties of the semifield are made. Then we focus on three different cases. We end this section with the BEL-construction.

In what follows $\mathrm{PG}(k, q)$ will denote the k-dimensional projective space over the finite field $\mathbb{F}_q$ with q elements. An *n-spread* of a projective space is a partition of the points of the space by subspaces of projective dimension n. From the theory developed by André [5], Bruck and Bose [13] it follows that the study of translation planes is equivalent to the study of $(n-1)$-spreads of $\mathrm{PG}(2n-1, q)$. The spreads that correspond to semifield planes in this way, are called *semifield spreads*. A spread of $\mathrm{PG}(2n-1, q)$ is called *symplectic* if there exists a nondegenerate alternating bilinear form $(\cdot, \cdot) : \mathbb{F}_q^n \oplus \mathbb{F}_q^n \to \mathbb{F}_q$ such that $(U, U) = 0$ for each spread element $\mathrm{PG}(U)$. If a semifield spread is symplectic, then the associated semifield is called *symplectic* too.

In general, one can construct a design from an arbitrary spread; if the design is isomorphic to a Desarguesian projective space (i.e. a Desarguesian projective plane or a projective space of dimension at least 3), then the spread is called a *Desarguesian spread*.

A set L of points in $\mathrm{PG}(r-1, q_0)$ is called a *linear set* if there exists a subspace U in $\mathrm{PG}(rt-1, q)$, for some $t \geq 1$, $q^t = q_0$, such that L is the set of points corresponding to the elements of a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1, q)$ intersecting U. (We denote this by $L = B(U)$.) If we want to specify the field $\mathbb{F}_q$ over which L is linear, we call L an *$\mathbb{F}_q$-linear set*. If U has dimension d in $\mathrm{PG}(rt-1, q)$, then the linear set $B(U)$ is called a linear set *of rank* $d+1$.

The same notation and terminology is used when U is a subspace of the vector space $V(rt, q)$ instead of a projective subspace. For an overview of the use of linear sets in various other areas of Finite Geometry, we refer to [43], [50], and [62].

Let $\mathbb{S}$ be an n-dimensional semifield over $\mathbb{F}_q$, and as before denote the dimensions of $\mathbb{S}$ over its nuclei by l, m and r. The spread corresponding to the semifield plane $\pi(\mathbb{S})$ can also be constructed algebraically from the coordinatising semifield, see e.g. [30]. (In order to avoid unnecessary generality, we restrict ourselves to the case where π is a semifield plane, but the construction holds for each translation plane.) There are essentially two approaches one can take, by considering either the endomorphisms L_x or R_x. In the literature it is common to use the endomorphism R_x. We define the following subspaces of $\mathbb{S} \times \mathbb{S}$. For each $x \in \mathbb{S}$, consider the set of vectors $S_x := \{(y, y^{R_x}) : y \in \mathbb{S}\}$, and put $S_\infty := \{(0, y) : y \in \mathbb{S}\}$. It is an easy exercise to show that $\mathcal{S} := \{S_x : x \in \mathbb{S}\} \cup \{S_\infty\}$ is a spread of $\mathbb{S} \times \mathbb{S}$. The set of endomorphisms $\mathcal{R} := \{R_x : x \in \mathbb{S}\} \subset \mathrm{End}(V_l(\mathbb{S}))$ is called the *semifield spread set* corresponding to $\mathbb{S}$. Note that by (S2) the spread set $\mathcal{R}$ is closed under addition and, by (S3), the non-zero elements of $\mathcal{R}$ are invertible.

This means that n-dimensional semifields over $\mathbb{F}_q$, can be investigated via the $\mathbb{F}_q$-vector space $U \subset \mathbb{F}_q^{ln}$ of dimension n induced by the $\mathbb{F}_q$-vector space $\mathcal{R} \subset \mathrm{End}(V_l(\mathbb{S}))$. Projectively this corresponds to the study of the $\mathbb{F}_q$-linear set $L(\mathbb{S}) := B(U)$ of rank n in $\mathrm{PG}(l^2-1, q^{n/l}) = \mathrm{PG}(V_l(\mathbb{S}))$.

Since $\mathbb{S}$ has no zero divisors, each R_x is nonsingular, and hence the linear set $L(\mathbb{S})$ is disjoint from the $(l-2)$nd secant variety of the Segre variety in $\mathrm{PG}(l^2-1, q^{n/l})$.

Let $\mathcal{S}_{l,l}(q^{n/l})$ denote the Segre variety in $\mathrm{PG}(l^2-1, q^{n/l})$, and denote its $(l-2)$nd secant variety by Ω. Furthermore let $\mathcal{G}$ denote the stabiliser inside the collineation group $\mathrm{P\Gamma L}(l^2, q^{n/l})$ of the two families of maximal subspaces on $\mathcal{S}_{l,l}(q^{n/l})$, and let X denote the set of linear sets of rank n disjoint from Ω.

3.1. **The general case.**

If we don't make any further assumptions on the sizes of the nuclei, then we have the following theorem from [47].

Theorem 3.1. *There is a one-to-one correspondence between the isotopism classes of semifields of order q^n, l-dimensional over their left nucleus and the orbits of $\mathcal{G}$ on the set X.*

This also holds if we replace the left nucleus by a subfield of the left nucleus. In particular if we consider the semifield over (a subfield of) its nucleus, then in the statement of the theorem the linear sets are replaced by the subspaces and we have the following from [46].

Theorem 3.2. *Let $\mathcal{G}$ denote the stabiliser inside the collineation group $\mathrm{P\Gamma L}(n^2, q)$ of the two families of maximal subspaces on $\mathcal{S}_{n,n}(q)$, and let Ω denote the $(n-2)$nd secant variety of $\mathcal{S}_{n,n}(q)$. There is a one-to-one correspondence between the isotopism classes of n-dimensional semifields over $\mathbb{F}_q$ and the orbits of the group $\mathcal{G}$ on the set of $(n-1)$-dimensional subspaces disjoint from Ω.*

3.2. **Rank two semifields.**

In this case we assume that the left nucleus has size the square root of the size of the semifield, i.e. $l = 2$. Then $L(\mathbb{S})$ becomes an $\mathbb{F}_q$-linear set in $\mathrm{PG}(3, q^{n/2})$ of rank n disjoint from a hyperbolic quadric, and the study of the isotopism classes corresponds to the study of these linear sets with respect to the collineation group fixing the reguli of the hyperbolic quadric (see [16]).

Rank two semifields have been studied extensively (see for instance the classification results mentioned above). One of the features of rank two semifields is that they allow an extension of the Knuth orbit. Using the polarity associated to the hyperbolic quadric, one obtains the so-called *translation dual* ([53]) $\mathbb{S}^\perp$ of $\mathbb{S}$, and this generates a set of possibly twelve isotopism classes $\mathcal{K}(\mathbb{S}) \cup \mathcal{K}(\mathbb{S}^\perp)$. We refer to [48, Section 3] for further details and references.

3.3. **Symplectic or commutative semifields.**

In this case we assume that the isotopism class of $\mathbb{S}$ contains a semifield that is commutative. If $\mathbb{S}$ is commutative, then the structure constants satisfy the property $a_{ijk} = a_{jik}$. By definition, the structure constants of $\mathbb{S}^{dt}$ are $b_{ijk} = a_{ikj}$, and hence the matrix $(a_{ikj})_{ik}$ of right multiplication by e_j in $\mathbb{S}^{dt}$ is symmetric. Choosing the right bilinear form it follows that the spread is symplectic leading to the following correspondence (see [35]).

Theorem 3.3. *A pre–semifield $\mathbb{S}$ is symplectic if and only if the pre–semifield $\mathbb{S}^{dt}$ is isotopic to a commutative semifield.*

This implies that in the study of the Knuth orbit, commutative semifields and symplectic semifields play an equivalent role. However, note that being symplectic is well defined up to isotopism, while commutativity is not.

The following theorem from [54] gives a very nice geometric characterization of symplectic semifields.

Theorem 3.4. *A pre-semifield $\mathbb{S}$ is symplectic if and only if $L(\mathbb{S})$ is contained in an $(\frac{l^2+l}{2}-1)$-dimensional subspace intersecting $\mathcal{S}_{l,l}(q^{n/l})$ in a Veronese variety $\mathcal{V}_l(q^{n/l})$.*

In odd characteristic, commutative semifields are of special interest in differential cryptanalysis, due to there connections to perfect nonlinear functions (PN). In even characteristic they are connected with $\mathbb{Z}_4$-linear codes and extremal line sets in Euclidean spaces. See [48, Section 4] for further references.

Now, if $\mathbb{S}$ is a symplectic semifield which is three-dimensional over its left nucleus ($l=3$) then the linear set is contained in a 5-dimensional space intersecting $\mathcal{S}_{3,3}(q^{n/3})$ in a Veronesean surface. Also in this case the Knuth orbit can be extended; this time using the polarity of $\mathrm{PG}(5, q^{n/3})$ that sends tangents planes to conic planes of $\mathcal{V}_3$, see [54]. The new semifield is called the *symplectic dual*. In the same paper, the authors establish the interesting fact that the symplectic dual of a field gives a twisted field ([54, Theorem 4]).

3.4. **Rank Two Commutative Semifields (RTCS).**

The combination of the previous two cases give us the type of semifields that play an important role in finite geometry. It follows from the above that in this case $L(\mathbb{S})$ is contained in a plane intersecting $Q^+(3, q^{n/2})$ in a conic. A complete classification or new examples would be very interesting from many points of view. We refer to [48, Section 5] for further details.

3.5. **The BEL-construction.**

In this section we concentrate on a geometric construction of finite semifield spreads. The construction we give here is taken from [47], but the main idea is the slightly less general construction given in [9] (where L is a subspace, i.e. $t=1$). We will refer to this construction as the *BEL-construction*.

We define a *BEL-configuration* as a triple $(\mathcal{D}, U, W)$, where $\mathcal{D}$ a Desarguesian $(n-1)$-spread of $\Sigma_1 := \mathrm{PG}(rn-1, s^t)$, $t \geq 1$, $r \geq 2$; U is an nt-dimensional subspace of $\mathbb{F}_s^{rnt}$ such that $L = B(U)$ is an $\mathbb{F}_s$-linear set of Σ_1 of rank nt; and W is a subspace of Σ_1 of dimension $rn-n-1$, such that no element of $\mathcal{D}$ intersects both L and W. From a BEL-configuration one can construct a semifield spread as follows.

- Embed Σ_1 in $\Lambda_1 \cong \mathrm{PG}(rn+n-1, s^t)$ and extend $\mathcal{D}$ to a Desarguesian spread $\mathcal{D}_1$ of Λ_1.
- Let $L' = B(U')$, $U \subset U'$ be an $\mathbb{F}_s$-linear set of Λ_1 of rank $nt+1$ which intersects Σ_1 in L.
- Let $\mathcal{S}(\mathcal{D}, U, W)$ be the set of subspaces defined by L' in the quotient geometry $\Lambda_1/W \cong \mathrm{PG}(2n-1, s^t)$ of W, i.e.,

$$\mathcal{S}(\mathcal{D}, U, W) = \{\langle R, W\rangle/W \ : \ R \in \mathcal{D}_1, R \cap L' \neq \emptyset\}.$$

Theorem 3.5 ([47]). *The set $\mathcal{S}(\mathcal{D}, U, W)$ is a semifield spread of* $\mathrm{PG}(2n-1, s^t)$. *Conversely, for every finite semifield spread $\mathcal{S}$, there exists a BEL-configuration $(\mathcal{D}, U, W)$, such that $\mathcal{S}(\mathcal{D}, U, W) \cong \mathcal{S}$.*

The pre-semifield corresponding to $\mathcal{S}(\mathcal{D}, U, W)$ is denoted by $\mathbb{S}(\mathcal{D}, U, W)$. Using this BEL-construction it is not difficult to prove the following characterisation of the linear sets corresponding to a finite field.

Theorem 3.6 ([46]). *The linear set $L(\mathbb{S})$ of* $\mathrm{PG}(n^2-1, q)$ *disjoint from $\Omega(\mathcal{S}_{n,n})$ corresponds to a pre–semifield isotopic to a field if and only if there exists a Desarguesian $(n-1)$–spread of* $\mathrm{PG}(n^2-1, q)$ *containing $L(\mathbb{S})$ and a system of maximal subspaces of $\mathcal{S}_{n,n}$.*

If $r = 2$ and $t = 1$, then we can use the symmetry in the definition of a BEL-configuration to construct two semifields, namely $\mathbb{S}(\mathcal{D}, U, W)$ and $\mathbb{S}(\mathcal{D}, W, U)$, and in this way we can extend the Knuth orbit by considering the operation (called *switching*)

$$\kappa := \mathbb{S}(\mathcal{D}, U, W) \mapsto \mathbb{S}(\mathcal{D}, W, U). \tag{11}$$

It is known that the switching process is a nontrivial extension of the Knuth orbit (see [44, Remark 3.1], [37, Section 5]), but - except in the case where the semifield is a rank two semifield (see Section 3.2), in which case κ becomes the translation dual (see [53]) - it is not known whether κ is well defined on the set of isotopism classes.

4. A tensor product approach to finite semifields

This coordinate free approach to semifields is based on Liebler [52] relying on results obtained by Cronheim [19]. Here we give a proof of the correspondence between semifields and nonsingular tensors without relying on [19], and elaborate on this approach. We end this section with a geometric condition for nonsingularity.

4.1. **Contractions and nonsingular tensors.**

Consider the tensor product $\bigotimes_{i\in I} V_i$ ($I = \{1, \ldots, r\}$), with $\mathrm{dim}V_i = n_i$. The elements $u \in \bigotimes_{i\in I} V_i$ that can be written as

$$u = v_1 \otimes \ldots \otimes v_r$$

for some $v_1 \in V_1, \ldots, v_r \in V_r$, are called the *fundamental tensors* or *pure tensors*. The set of fundamental tensors generates the whole vector space $\bigotimes_{i\in I} V_i$. If $u = v_1 \otimes \ldots \otimes v_r$ is a fundamental tensor in $\bigotimes_{i\in I} V_i$, and $v_i^\vee \in V_i^\vee$, where $V_i^\vee$ denotes the dual space of V_i, then we define $v_i^\vee(u)$ as the tensor

$$v_i^\vee(u) := v_i^\vee(v_i)(v_1 \otimes \ldots \otimes v_{i-1} \otimes v_{i+1} \otimes \ldots \otimes v_r) \in \bigotimes_{j\in I\setminus\{i\}} V_j. \tag{12}$$

Since the fundamental tensors span $\bigotimes_{i\in I} V_i$, this definition naturally extends to a definition of $v_i^\vee(v)$ for any $v \in \bigotimes_{i\in I} V_i$. We call

$$v_i^\vee(v) \in \bigotimes_{j\in I\setminus\{i\}} V_j,$$

the *contraction of $v \in \bigotimes_{i\in I} V_i$ by $v_i^\vee \in V_i^\vee$*. Also, we say that a nonzero vector of V_i is *nonsingular*, and by induction that a tensor $v \in \bigotimes_{i\in I} V_i$ is *nonsingular* if for every $i \in I$

and $v_i^\vee \in V_i^\vee$, $v_i^\vee \neq 0$, the contraction $v_i^\vee(v)$ is nonsingular. Note that this definition is in agreement with the definition of nonsingular hypercubes given in [42].

Before we continue with our study of the nonsingular tensor attached to a semifield, we make a few more general observations. Let T be a nonsingular tensor in $\bigotimes_{1\leq i\leq r} V_i$. Define

$$E_i := \langle v_i^\vee(T) \ : \ v_i^\vee \in V_i^\vee \rangle \tag{13}$$

i.e., E_i is the subspace spanned by the contractions of T by the elements of $V_i^\vee$.

Lemma 4.1. *Each E_i has dimension n_i and every non-zero element of E_i is a nonsingular tensor.*

Proof. Clearly, each E_i has dimension at most n_i. Suppose E_i has dimension less than n_i. Then there exists a non-trivial linear combination of linearly independent elements $e_{i1}^\vee, \ldots, e_{in_i}^\vee$ of $V_i^\vee$:

$$a_1 e_{i1}^\vee(T) + \ldots + a_{n_i} e_{in_i}^\vee(T) = 0,$$

with $a_1, \ldots, a_n \in \mathbb{F}$ not all zero. But this implies that the contraction $w^\vee(T) = 0$, with $0 \neq w^\vee = a_1 e_{i1}^\vee + \ldots + a_{n_i} e_{in_i}^\vee \in V_i^\vee$. This means that T is singular, a contradiction.

Next choose any $0 \neq u \in E_i$. By definition u is a linear combination of contractions of T by elements of $V_i^\vee$, and hence u is a contraction itself. Since T is nonsingular, u must be nonsingular too. □

This means that every nonsingular tensor gives a subspace of nonsingular tensors in the tensor product with one of the factors left out. The dimension of this subspace equals the dimension of the factor that is left out.

4.2. **Nonsingular tensors and semifields.** Consider an n-dimensional presemifield $\mathbb{S}$ over its center $\mathbb{F} = \mathbb{F}_q$, and multiplication $x \circ y$. We denote by

$$T_{\mathbb{S}} \in V^\vee \otimes V^\vee \otimes V \tag{14}$$

the element of $V^\vee \otimes V^\vee \otimes V$ (with $V = \mathbb{F}^n$, and $V^\vee$ the dual space of V) defined as follows. Let $h_{\mathbb{S}} \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)$ denote the homomorphism defined by $\circ \ : \ V \times V \to V$ and the universal property of the tensor product. In other words $h_{\mathbb{S}}$ is defined by the following diagram.

$$\begin{tikzcd}
V \times V \arrow[rr, "x \circ y"] \arrow[dr] & & V \\
& V \otimes V \arrow[ur, "h_{\mathbb{S}} \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)"'] &
\end{tikzcd}$$

Figure 3. The homomorphism $h_{\mathbb{S}}$ defined by $\mathbb{S}$

Also, consider the isomorphism

$$\varphi : V^\vee \otimes V^\vee \otimes V \to \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V) \tag{15}$$

defined by

$$(v_1 \otimes v_2)(u^\vee \otimes v^\vee \otimes w)^\varphi := u^\vee(v_1)v^\vee(v_2)w.$$

We define $T_{\mathbb{S}}$ as the pre-image of $h_{\mathbb{S}}$ under φ, i.e. $T_{\mathbb{S}}^\varphi = h_{\mathbb{S}}$. For future reference we remark that the inverse image of $h \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)$ under φ^{-1} is given by

$$h^{\varphi^{-1}} = \sum_{i,j} \left[e_i^\vee \otimes e_j^\vee \otimes h(e_i \otimes e_j) \right] \in V^\vee \otimes V^\vee \otimes V \tag{16}$$

where $\{e_l\}$ is a basis for V and $\{e_l^\vee\}$ is the dual basis for $V^\vee$. For our convenience, we denote $V_1 = V_2 = V^\vee$ and $V_3 = V$. Note that $T^\varphi = h$ implies that for any $v_1^\vee \in V_1^\vee$, $v_2^\vee \in V_2^\vee$ we have

$$v_1^\vee(v_2^\vee(T)) = \sum_{k,l} w_1(e_k^\vee)w_2(e_l^\vee)h(e_k \otimes e_l) = \sum_{k,l} w_{1k}w_{2l}h(e_k \otimes e_l) = h(w_1 \otimes w_2),$$

where $v_i^\vee = w_i = (w_{i1}, \ldots, w_{in})$ for $i = 1, 2$, with respect to the basis $\{e_l\}$ for $V_1^\vee = V_2^\vee = V$, and hence for any $T \in V_1 \otimes V_2 \otimes V_3$ the following holds:

$$\forall v_1^\vee \in V_1^\vee, \forall v_2^\vee \in V_2^\vee \ : \ v_1^\vee(v_2^\vee(T)) = T^\varphi(v_1^\vee \otimes v_2^\vee). \tag{17}$$

We also define the functional isomorphisms

$$\varphi_{ij} \ : \ V_i \otimes V_j \to \mathrm{Hom}_{\mathbb{F}}(V_i^\vee, V_j) \ : \ (v_i \otimes v_j)^{\varphi_{ij}} \ : \ v_i^\vee \mapsto v_i^\vee(v_i)v_j. \tag{18}$$

We have the following correspondence between nonsingular tensors and pre-semifields.

Theorem 4.2. (i) *The tensor $T_{\mathbb{S}} \in V_1 \otimes V_2 \otimes V_3$ is nonsingular.*
(ii) *To every nonsingular tensor $T \in V_1 \otimes V_2 \otimes V_3$ there corresponds a presemifield $\mathbb{S}$ for which $T = T_{\mathbb{S}}$.*
(iii) *The map $\mathbb{S} \mapsto T_{\mathbb{S}}$ is injective.*

Proof. (i) If $T_{\mathbb{S}}$ is singular, there exists a $v_i^\vee \neq 0$ in $V_i^\vee$ for which the contraction $v_i^\vee(T_{\mathbb{S}})$ of $T_{\mathbb{S}}$ is singular, which in turn implies that there exists a $v_j^\vee \in V_j^\vee$, $j \neq i$, for which $v_j^\vee(v_i^\vee(T_{\mathbb{S}})) = 0$. Since the contractions $v_j^\vee(v_i^\vee(T_{\mathbb{S}}))$ and $v_i^\vee(v_j^\vee(T_{\mathbb{S}}))$ are equal we may assume that $i > j$.

If $(i, j) = (2, 1)$, then by using (17) we obtain $h_{\mathbb{S}}(v_1^\vee \otimes v_2^\vee) = 0$.

Next suppose $i = 3$. Using (18), $v_3^\vee(T_{\mathbb{S}}) \in V_1 \otimes V_2$ is singular if and only if $(v_3^\vee(T_{\mathbb{S}}))^{\varphi_{12}} \in \mathrm{Hom}_{\mathbb{F}}(V_1^\vee, V_2)$ has a nontrivial kernel. Equivalently, there exists a $w_1 = v_1^\vee \in V_1^\vee$, such that

$$V^\vee = V_2 \ni 0 = (v_3^\vee(T_{\mathbb{S}}))^{\varphi_{12}}(w_1) = \sum_{k,l} [v_3^\vee(h_{\mathbb{S}}(e_k \otimes e_l)) \ (e_k^\vee \otimes e_l^\vee)^{\varphi_{12}}(w_1)]$$

$$= \sum_{k,l} v_3^\vee(h_{\mathbb{S}}(e_k \otimes e_l)) \ w_1(e_k^\vee)e_l^\vee = \sum_{k,l} v_3^\vee(h_{\mathbb{S}}(e_k \otimes e_l)) \ w_{1k}e_l^\vee = \sum_{l} v_3^\vee(h_{\mathbb{S}}(w_1 \otimes e_l)) \ e_l^\vee.$$

This implies that

$$\forall l \ : \ v_3^\vee(h_{\mathbb{S}}(w_1 \otimes e_l)) = 0 \in \mathbb{F}.$$

Since $v_3^\vee \neq 0$, it follows that the dimension of $\langle h_{\mathbb{S}}(w_1 \otimes e_1), h_{\mathbb{S}}(w_1 \otimes e_2), \ldots, h_{\mathbb{S}}(w_1 \otimes e_n) \rangle$ is at most $n - 1$. Hence, there exist $a_1, a_2, \ldots, a_n \in \mathbb{F}$, not all a_i zero, for which

$$a_1 h_{\mathbb{S}}(w_1 \otimes e_1) + a_2 h_{\mathbb{S}}(w_1 \otimes e_2) + \ldots + a_n h_{\mathbb{S}}(w_1 \otimes e_n) = 0.$$

Using the linearity of $h_{\mathbb{S}}$ this implies that

$$h_{\mathbb{S}}(w_1 \otimes (a_1 e_1 + a_2 e_2 + \ldots + a_n e_n)) = 0,$$

with $a_1 e_1 + a_2 e_2 + \ldots + a_n e_n \neq 0$.

Summarizing, we have shown that if $T_{\mathbb{S}}$ is singular, then there exist nonzero $u \otimes v \in V \otimes V$, for which $h_{\mathbb{S}}(u \otimes v) = 0$, and hence $u \circ v = 0$. This contradicts the property that a presemifield has no zero divisors.

(ii) Define a multiplication $\circ : V \times V \to V$ by

$$x \circ y := T^{\varphi}(x \otimes y), \text{ for } x, y \in V, \tag{19}$$

and consider the algebraic structure $\mathbb{S} = V, +, \circ$. Clearly $(\mathbb{S}, +)$ is elementary abelian, and since $T^{\varphi} \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V)$, both distributive laws are satisfied in $\mathbb{S}$. We verify that $\mathbb{S}$ has no zero divisors. To that extend suppose $x \circ y = 0$, with $x \neq 0 \neq y$. Then

$$0 = T^{\varphi}(x \otimes y) = x(y(T)),$$

by (17). This implies that the contraction $x(y(T)) = 0 \in V_3$, and hence that T is singular, a contradiction.

(iii) If $T_{\mathbb{S}_1} = T_{\mathbb{S}_2}$, then $x \circ_1 y = T^{\varphi}_{\mathbb{S}_1}(x \otimes y) = T^{\varphi}_{\mathbb{S}_2}(x \otimes y) = x \circ_2 y$, for all $x, y \in V$. □

4.3. **The isotopism classes.** Denote by $\mathcal{G}$ the group $\mathrm{GL}(V_1) \times \mathrm{GL}(V_2) \times \mathrm{GL}(V_3)$ with its natural action on $V_1 \otimes V_2 \otimes V_3$ defined by its action on the fundamental tensors:

$$(g_1, g_2, g_3) \ : \ v_1 \otimes v_2 \otimes v_3 \mapsto v_1^{g_1} \otimes v_2^{g_2} \otimes v_3^{g_3}. \tag{20}$$

Then we have the following theorem.

Theorem 4.3. *Two presemifields $\mathbb{S}_1$ and $\mathbb{S}_2$ are isotopic if and only $T^{\mathcal{G}}_{\mathbb{S}_1} = T^{\mathcal{G}}_{\mathbb{S}_2}$.*

Proof. Suppose that an isotopism between $\mathbb{S}_1$ and $\mathbb{S}_2$ is given by

$$x^F \circ_2 y^G = (x \circ_1 y)^H,$$

where F, G, and H are nonsingular linear transformations from $\mathbb{S}_1$ to $\mathbb{S}_2$. We claim that

$$T_{\mathbb{S}_2}^{(F^{\vee}, G^{\vee}, H^{-1})} = T_{\mathbb{S}_1},$$

where $F^{\vee} \in \mathrm{GL}(V_1)$ denotes the action induced on $V_1 = V^{\vee}$ by $F \in \mathrm{GL}(V)$, defined as follows: $\forall w^{\vee} \in V^{\vee}$ we define

$$F^{\vee} \in \mathrm{GL}(V^{\vee}) \ : \ w^{\vee} \ \mapsto \ \left[(w^{\vee})^{F^{\vee}} \in V^{\vee} \ : \ v \ \mapsto w^{\vee}(v^F) \right]. \tag{21}$$

Note that this implies that $\{(e_i^{\vee})^{F^{\vee}}\}$ is the dual basis of $\{e_i^{F^{-1}}\}$, and similar for G. To prove the claim, consider the images of the elements of the basis $\{e_i^{F^{-1}} \otimes e_j^{G^{-1}}\}$ of $V \otimes V$ under the homomorphism

$$\left(T_{\mathbb{S}_2}^{(F^{\vee}, G^{\vee}, H^{-1})} \right)^{\varphi} \in \mathrm{Hom}_{\mathbb{F}}(V \otimes V, V) :$$

$$e_i^{F^{-1}} \otimes e_j^{G^{-1}} \ \mapsto \ \sum_{k,l} (e_k^{\vee})^{F^{\vee}} (e_i^{F^{-1}}) \ (e_l^{\vee})^{G^{\vee}} (e_j^{G^{-1}}) \ \left(h_{\mathbb{S}_2}(e_k \otimes e_l) \right)^{H^{-1}} = \left(h_{\mathbb{S}_2}(e_i \otimes e_j) \right)^{H^{-1}}.$$

Since φ is an isomorphism, and

$$T^{\varphi}_{\mathbb{S}_1}(e_i^{F^{-1}} \otimes e_j^{G^{-1}}) = h_{\mathbb{S}_1}(e_i^{F^{-1}} \otimes e_j^{G^{-1}}) = \left(h_{\mathbb{S}_2}(e_i \otimes e_j) \right)^{H^{-1}},$$

the claim is proved.

Conversely, if $T_{\mathbb{S}_1}^{\mathcal{G}} = T_{\mathbb{S}_2}^{\mathcal{G}}$, say $T_{\mathbb{S}_2}^{g} = T_{\mathbb{S}_1}$ with $g = (F^\vee, G^\vee, H^{-1}) \in \mathcal{G}$, then

$$\begin{aligned}(e_i \circ_2 e_j)^{H^{-1}} &= (h_{\mathbb{S}_2}(e_i \otimes e_j))^{H^{-1}} = \left(T_{\mathbb{S}_2}^{g}\right)^{\varphi}(e_i^F \otimes e_j^G)\\ &= (T_{\mathbb{S}_1})^{\varphi}(e_i^F \otimes e_j^G) = h_{\mathbb{S}_1}(e_i^F \otimes e_j^G) = e_i^F \circ_1 e_j^G,\end{aligned}$$

where $\{e_i\}$ is a basis for V. This implies that we have an isotopism between $\mathbb{S}_1$ and $\mathbb{S}_2$ given by

$$x^F \circ_2 y^G = (x \circ_1 y)^H.$$

□

Remark 4.4. *From the proof we extract the following correspondence:*

$$(F, G, H) \ : \ \mathbb{S}_1 \mapsto \mathbb{S}_2 \ \Leftrightarrow \ (F^\vee, G^\vee, H^{-1}) \ : \ T_{\mathbb{S}_1} \mapsto T_{\mathbb{S}_2}. \tag{22}$$

This theorem gives a one-to-one correspondence between the set of isotopism classes of n-dimensional semifields over $\mathbb{F}_q$ and the $\mathcal{G}$-orbits of nonsingular tensors in $V_1 \otimes V_2 \otimes V_3$:

$$[\mathbb{S}] \leftrightarrow T_{\mathbb{S}}^{\mathcal{G}}.$$

Moreover we have the following.

Theorem 4.5. *The autotopism group of a semifield $\mathbb{S}$ is isomorphic to the stabiliser of $T_{\mathbb{S}}$ in $\mathcal{G}$.*

Proof. Immediately from (22). □

4.4. **Non-singular tensors and Segre varieties.** In this section we explain the connections between a nonsingular tensor $T_{\mathbb{S}}$ associated to a semifield $\mathbb{S}$ and Segre varieties. We start with some general definitions and observations.

A *Segre variety* is usually defined as the image of the *Segre embedding*; an injective map from the product of projective spaces $\mathrm{PG}(V_1) \times \mathrm{PG}(V_2) \times \ldots \times \mathrm{PG}(V_r)$ into the projective space $\mathrm{PG}(\bigotimes_{i \in I} V_i)$. The image is an algebraic variety consisting of the points that correspond to the fundamental tensors in $\bigotimes_{i \in I} V_i$. We denote this variety by $\mathcal{S}_{n_1,\ldots,n_r}$, where $n_i = \mathrm{dim} V_i$, $i = 1, \ldots, r$. The subspaces of maximal dimension that are contained in $\mathcal{S}_{n_1,\ldots,n_r}$ are called the *maximal subspaces of* $\mathcal{S}_{n_1,\ldots,n_r}$, and they are partitioned into r *families* $\mathcal{M}_1, \ldots, \mathcal{M}_r$ *of maximal subspaces.* Each element of the family $\mathcal{M}_i$ has dimension n_i and each point $\langle (v_1 \otimes \ldots \otimes v_r) \rangle$ that lies on the variety $\mathcal{S}_{n_1,\ldots,n_r}$ is contained in exactly one member

$$\mathrm{PG}(v_1 \otimes \ldots \otimes v_{i-1} \otimes V_i \otimes v_{i+1} \ldots \otimes v_r) \in \mathcal{M}_i,$$

$(i = 1, \ldots, r)$ of each of these families.

Let us denote the point of $\mathrm{PG}(V_1 \otimes V_2 \otimes V_3)$ defined by a nonsingular tensor $T_{\mathbb{S}} \in V_1 \otimes V_2 \otimes V_3$ associated to a semifield $\mathbb{S}$ by $P_{\mathbb{S}}$, i.e.

$$P_{\mathbb{S}} := \mathrm{PG}(\langle T_{\mathbb{S}} \rangle) \in \mathrm{PG}(V_1 \otimes V_2 \otimes V_3).$$

Theorem 4.6. *If $P_{\mathbb{S}_1} = P_{\mathbb{S}_2}$, then $[\mathbb{S}_1] = [\mathbb{S}_2]$.*

Proof. If $P_{\mathbb{S}_1} = P_{\mathbb{S}_2}$, then there exists an $a \in \mathbb{F}$, $a \neq 0$, such that $T_{\mathbb{S}_1} = aT_{\mathbb{S}_2}$. By Remark 4.4, the triple $(id, id, x \mapsto a^{-1}x)$ defines an isotopism between $\mathbb{S}_1$ and $\mathbb{S}_2$. □

If we denote by $\mathcal{H}$ the subgroup of $\mathrm{PGL}(V_1 \otimes V_2 \otimes V_3)$ induced by $\mathcal{G} \leq \mathrm{GL}(V_1 \otimes V_2 \otimes V_3)$, then we obtain the following.

Theorem 4.7. *Two semifields $\mathbb{S}_1$ and $\mathbb{S}_2$ are isotopic if and only if $P_{\mathbb{S}_1}^{\mathcal{H}} = P_{\mathbb{S}_2}^{\mathcal{H}}$.*

Proof. Suppose $\mathbb{S}_1$ and $\mathbb{S}_2$ are isotopic. By Theorem 4.3 this is equivalent to $T_{\mathbb{S}_1}^{\mathcal{G}} = T_{\mathbb{S}_2}^{\mathcal{G}}$. By the definition of $\mathcal{H}$ the latter is equivalent to $P_{\mathbb{S}_1}^{\mathcal{H}} = P_{\mathbb{S}_2}^{\mathcal{H}}$. □

The group $\mathcal{H}$ is the subgroup of the setwise stabiliser in $\mathrm{PGL}(V_1 \otimes V_2 \otimes V_3)$ of the points on the Segre variety $\mathcal{S}_{n,n,n}(q)$, which leaves invariant the families of maximal subspaces of $\mathcal{S}_{n,n,n}(q)$.

Definition 4.8. *We define the* projective autotopism group *of a semifield $\mathbb{S}$ as the stabiliser of $P_{\mathbb{S}}$ in $\mathcal{H}$.*

4.5. **The tensor rank of a semifield.** Since the group $\mathcal{G}$ preserves the rank of a tensor, it is natural to introduce the following definition.

Definition 4.9. *We define the* tensor rank *of a semifield $\mathbb{S}$ as the rank of the corresponding tensor $T_{\mathbb{S}}$, and denote the tensor rank of $\mathbb{S}$ by* $\mathrm{Trk}(\mathbb{S})$.

From the above we immediately obtain an invariant.

Theorem 4.10. *The tensor rank* Trk *is an invariant for the isotopism classes of semifields.*

Proof. If $\mathbb{S}_1$ and $\mathbb{S}_2$ are isotopic, with an isotopism given by (F, G, H), then from (22) it follows that $(F^\vee, G^\vee, H^{-1})$ maps $T_{\mathbb{S}_1}$ to $T_{\mathbb{S}_2}$. If

$$T_{\mathbb{S}_1} = \sum_i u_i \otimes v_i \otimes w_i$$

then

$$T_{\mathbb{S}_2} = \sum_i u_i^{F^\vee} \otimes v_i^{G^\vee} \otimes w_i^{H^{-1}}.$$

Since F, G, and H are nonsingular, it follows that the rank of $T_{\mathbb{S}_1}$ and $T_{\mathbb{S}_2}$ are the same. This implies that $\mathrm{Trk}(\mathbb{S}_1) = \mathrm{Trk}(\mathbb{S}_2)$. □

4.6. **The Knuth orbit.** The Knuth orbit of a semifield $\mathbb{S}$ is the set of isotopism classes obtained from the semifield $\mathbb{S}$ by permuting the indices of the structure constants with respect to a basis for $\mathbb{S}$. Geometrically the Knuth orbit is obtained by considering the dual semifield plane, the dual semifield spread, etc. However, the only Knuth derivative of a semifield $\mathbb{S}$ that is visible in the geometric approach using linear sets as explained in Section 3, is the linear set L corresponding to a pre-semifield isotopic to the transpose semifield $\mathbb{S}^t$. Namely, the linear set L is obtained from $L(\mathbb{S})$ by applying a collineation τ of the projective space $\mathrm{PG}(l^2-1, q^{n/l})$ such that τ stabilizes the set of points on the Segre variety $\mathcal{S}_{l,l}(q^{n/l})$, but interchanges the two families of maximal subspaces of $\mathcal{S}_{l,l}(q^{n/l})$.

In this approach using nonsingular tensors the Knuth orbit of a semifield $\mathbb{S}$ can be seen as an orbit under a subgroup of $\mathrm{P\Gamma L}(n^3, q)$, isomorphic to $Sym(3)$, of the $\mathcal{H}$-orbit $P_{\mathbb{S}}^{\mathcal{H}}$.

The action corresponds to the action of $Sym(3)$ on the factors of $V_1 \otimes V_2 \otimes V_3$. For a fundamental tensor $v_1 \otimes v_2 \otimes v_3$ we have

$$(v_1 \otimes v_2 \otimes v_3)^{(12)} = (v_2 \otimes v_1 \otimes v_3) \text{ and } (v_1 \otimes v_2 \otimes v_3)^{(13)} = (v_3 \otimes v_2 \otimes v_1),$$

which defines the action of $Sym(3)$ on the space $V_1 \otimes V_2 \otimes V_3$. Projectively this action defines a subgroup of $\mathrm{P\Gamma L}(n^3, q)$ permuting the three families of maximal subspaces of the Segre variety $\mathcal{S}_{n,n,n}(q)$. This can also be seen based on the fact that the stabiliser $\mathcal{N}$of the set of points on the Segre variety $\mathcal{S}_{n,n,n}(q)$ inside $\mathrm{PGL}(n^3, q)$ is induced by the wreath product of $\mathrm{GL}(\mathbb{F}^n)$ with $Sym(3)$. From the above we have the following.

Proposition 4.11. *The Knuth orbit of a semifield $\mathbb{S}$ is represented in the projective space $\mathrm{PG}(n^3 - 1, q)$ as the orbit of $P_{\mathbb{S}}$ under the group $\mathcal{N}$.*

An interesting aspect of the tensor rank of a semifield is that it is not only an invariant of the isotopism class, but also of the Knuth orbit.

Theorem 4.12. *The tensor rank of a semifield,* Trk*, is an invariant for the Knuth orbit of a semifield.*

Proof. Suppose $[\mathbb{S}_1]$ and $[\mathbb{S}_2]$ belong to the same Knuth orbit. By Proposition 4.11 it follows that $P_{\mathbb{S}_1}$ and $P_{\mathbb{S}_2}$ belong to the same orbit of $\mathcal{N}$. Since the action of $Sym(3)$ defined above does not change the tensor rank, the proof follows from Theorem 4.10. □

4.7. **BEL-configurations from a nonsingular tensor.** Let $\mathbb{S}$ be a semifield and consider the corresponding projective point $P_{\mathbb{S}} \in \mathrm{PG}(V_1 \otimes V_2 \otimes V_3)$ determined by the nonsingular tensor $T_{\mathbb{S}} \in V_1 \otimes V_2 \otimes V_3$. Consider the subspaces

$$U_{ij} := \langle v_k(T_{\mathbb{S}}) \ : \ v_k \in V_k^{\vee} \rangle \ \subset V_i \otimes V_j, \ i < j \tag{23}$$

defined as the span of the contractions of $T_{\mathbb{S}}$ by the elements of of $V_k^{\vee}$, $k \in \{1, 2, 3\} \setminus \{i, j\}$. Also define U_{ij}, $i > j$, as the subspaces of $V_i \otimes V_j$, obtained from U_{ji} by interchanging the two factors in each term, i.e., induced by the map $u \otimes v \mapsto v \otimes u$, defined on the fundamental tensors. It follows from above that U_{ij} has dimension n and projectively, we get the following.

Lemma 4.13. *Each subspace $\mathrm{PG}(U_{ij})$ is an $(n-1)$-dimensional subspace of $\mathrm{PG}(V_i \otimes V_j)$ disjoint from the $(n-2)$-th secant variety of the Segre variety $\mathcal{S}_{n,n}(q)$.*

Proof. The proof follows from Lemma 4.1 and the fact that nonsingular tensors in $\mathrm{PG}(U_{ij}) = \langle \mathcal{S}_{n,n}(q) \rangle$ correspond to points that are skew from the $(n-2)$-th secant variety of the Segre variety $\mathcal{S}_{n,n}(q)$. □

Hence from $P_{\mathbb{S}}$ we get six $(n-1)$-dimensional subspaces $\mathrm{PG}(U_{ij})$ disjoint from $\mathcal{S}_{n,n}^{(n-2)}(q)$, the $(n-2)$-th secant variety of the Segre variety $\mathcal{S}_{n,n}(q)$. These six subspaces $\mathrm{PG}(U_{ij})$ represent the isotopism classes of the Knuth orbit of $\mathbb{S}$. The isotopism class of each representative corresponds to the orbit of $\mathrm{PG}(U_{ij})$ under the subgroup of the stabilizer of the set of points on $\mathcal{S}_{n,n}(q)$ inside $\mathrm{PGL}(V_i \otimes V_j)$, fixing the two families of maximal subspaces of $\mathcal{S}_{n,n}(q)$.

Also, given a subspace $\mathrm{PG}(U)$ disjoint from $\mathcal{S}_{n,n}^{(n-2)}(q)$ associated to a semifield $\mathbb{S}$, we can reconstruct the nonsingular tensor $T_{\mathbb{S}}$ by choosing a basis $\{u_1, \ldots, u_n\}$ of U. The choice of the basis corresponds to the orbit of $T_{\mathbb{S}}$ under the subgroup id × id × $\mathrm{GL}(V)$ of $\mathcal{G}$ (or id × $\mathrm{GL}(V)$ × id or $\mathrm{GL}(V)$ × id × id, depending on the choices made) . From this nonsingular tensor one can then obtain the six subspaces $\mathrm{PG}(U_{ij})$, one of which being $\mathrm{PG}(U)$.

We conclude with the following geometric condition for nonsingularity.

Theorem 4.14. *Let $P = \langle T\rangle$ be a point in $\langle \mathcal{S}_{n,n,n}(q)\rangle = \mathrm{PG}(V_1 \otimes V_2 \otimes V_3)$. Then $T \in \bigotimes_{i\in I} V_i$ is singular, if and only if P is contained in a subspace $\langle x_1, \dots, x_j, S_{k_1,k_2,k_3}\rangle$ spanned by $j < n$ points x_i on the variety $\mathcal{S}_{n,n,n}$ and a Segre variety $\mathcal{S}_{k_1,k_2,k_3}$ properly contained in $\mathcal{S}_{n,n,n}$ (i.e. at least one $k_j < n$).*

Proof. If T is singular then there exists a contraction $v_i^\vee \in V_i^\vee$ such that $v_i^\vee(T)$ is singular. W.l.o.g. suppose $v_1^\vee(T) \in V_2 \otimes V_3$ is singular. Equivalently, there exists a hyperplane U_1 in V_1 such that $\langle v_1^\vee(T)\rangle$ is contained in the $(n-2)$nd secant variety of the Segre variety $\mathcal{S}_{n,n}$ induced by $\mathcal{S}_{n,n,n}$ and U_1 in $\mathrm{PG}(V_1 \otimes V_2 \otimes V_3/U_1 \otimes V_2 \otimes V_3)$, and hence there exist $n-1$ points $\bar{x}_i$ on $\mathcal{S}_{n,n}$ with

$$\langle v_1^\vee(T)\rangle \in \langle \bar{x}_1, \dots, \bar{x}_{n-1}\rangle.$$

In turn this implies the existence of $n-1$ points x_i on $\mathcal{S}_{n,n,n}$ such that

$$\bar{x}_i = \langle x_i, \mathrm{PG}(U_1 \otimes V_2 \otimes V_3)\rangle,\ i = 1, \dots, n-1.$$

If we denote the Segre variety induced by $\mathcal{S}_{n,n,n}$ in $\mathrm{PG}(U_1 \otimes V_2 \otimes V_3)$ by $\mathcal{S}_{n-1,n,n}$, then it follows that $P \in \langle x_1, \dots, x_{n-1}, \mathcal{S}_{n-1,n,n}\rangle$.

Conversely, suppose $P \in \langle x_1, \dots, x_j, \mathcal{S}_{k_1,k_2,k_3}\rangle$ spanned by $j < n$ points x_i on the variety $\mathcal{S}_{n,n,n}$ and a Segre variety $\mathcal{S}_{k_1,k_2,k_3}$ properly contained in $\mathcal{S}_{n,n,n}$. W.l.o.g. assume $k_1 \le n-1$. Consider a hyperplane U_1 in V_1, such that $\mathrm{PG}(U_1 \otimes V_2 \otimes V_3)$ contains $\mathcal{S}_{k_1,k_2,k_3}$. Put $t \le j$ equal to the minimal number of points $x_{i_1}, \dots, x_{i_t} \in \{x_1, \dots, x_j\}$ such that

$$\langle x_{i_1}, \dots, x_{i_t}, \mathrm{PG}(U_1 \otimes V_2 \otimes V_3)\rangle = \langle x_1, \dots, x_j, \mathrm{PG}(U_1 \otimes V_2 \otimes V_3)\rangle.$$

If $v_1^\vee(T)$ denotes the contraction corresponding to U_1, then

$$\langle v_1^\vee(T)\rangle \subset \langle \bar{x}_{i_1}, \dots, \bar{x}_{i_t}\rangle,$$

where

$$\bar{x}_{i_s} := \langle x_{i_s}, \mathrm{PG}(U_1 \otimes V_2 \otimes V_3)\rangle,\ s = 1, \dots, t.$$

It follows that the point $\langle v_1^\vee(T)\rangle$ is contained in the $(t-1)$th secant variety of the Segre variety (of type n, n) induced by $\mathcal{S}_{n,n,n}$ in $\mathrm{PG}(V_1 \otimes V_2 \otimes V_3/U_1 \otimes V_2 \otimes V_3)$. This implies that T is singular. □

Acknowledgement The author thanks Aart Blokhuis and Tim Penttila for interesting conversations on the subject, and the anonymous referees for their suggestions and remarks on the original version of the manuscript.

References

[1] A. A. Albert. Non-associative algebras. I. Fundamental concepts and isotopy. *Ann. of Math. (2)*, 43:685–707, 1942.

[2] A. A. Albert. On nonassociative division algebras. *Trans. Amer. Math. Soc.*, 72:296–309, 1952.

[3] A. A. Albert. Finite division algebras and finite planes. In *Proc. Sympos. Appl. Math., Vol. 10*, pages 53–70. American Mathematical Society, Providence, R.I., 1960.

[4] A. A. Albert. Generalized twisted fields. *Pacific J. Math.*, 11:1–8, 1961.

[5] J. André. Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. *Math. Z.*, 60:156–186, 1954.

[6] M. Aschbacher. Isotopy and geotopy for ternary rings of projective planes. *Journal of Algebra*, 319(2):868–892, 2008.

[7] L. Bader and G. Lunardon. On non-hyperelliptic flocks. *European J. Combin.*, 15(5):411–415, 1994.

[8] J. C. Baez. The octonions. *Bull. Amer. Math. Soc. (N.S.)*, 39(2):145–205, 2002.

[9] S. Ball, G. Ebert, and M. Lavrauw. A geometric construction of finite semifields. *J. Algebra*, 311(1):117–129, 2007.

[10] J. Bierbrauer. New semifields, PN and APN functions. *Des. Codes Cryptogr.*, 54(3):189–200, 2010.

[11] I. Bloemen, J. A. Thas, and H. Van Maldeghem. Translation ovoids of generalized quadrangles and hexagons. *Geom. Dedicata*, 72(1):19–62, 1998.

[12] A. Blokhuis, M. Lavrauw, and S. Ball. On the classification of semifield flocks. *Adv. Math.*, 180(1):104–111, 2003.

[13] R. H. Bruck and R. C. Bose. The construction of translation planes from projective spaces. *J. Algebra*, 1:85–102, 1964.

[14] R. H. Bruck and E. Kleinfeld. The structure of alternative division rings. *Proc. Amer. Math. Soc.*, 2:878–890, 1951.

[15] L. Budaghyan and T. Helleseth. New commutative semifields defined by new PN multinomials. *Cryptogr. Commun.*, 3(1):1–16, 2011.

[16] I. Cardinali, O. Polverino, and R. Trombetti. Semifield planes of order q^4 with kernel F_{q^2} and center F_q. *European J. Combin.*, 27(6):940–961, 2006.

[17] S. D. Cohen and M. J. Ganley. Commutative semifields, two-dimensional over their middle nuclei. *J. Algebra*, 75(2):373–385, 1982.

[18] R. S. Coulter and M. Henderson. Commutative presemifields and semifields. *Advances in Mathematics*, 217(1):282–304, 2008.

[19] A. Cronheim. T-groups and their geometry. *Illinois J. Math.*, 9:1–30, 1965.

[20] P. Dembowski. *Finite geometries.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 44. Springer-Verlag, Berlin, 1968.

[21] U. Dempwolff. Semifield planes of order 81. *J. Geom.*, 89(1-2):1–16, 2008.

[22] U. Dempwolff. On irreducible semilinear transformations. *Forum Math.*, 22(6):1193–1206, 2010.

[23] L. E. Dickson. Linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 7(3):370–390, 1906.

[24] L. E. Dickson. On commutative linear algebras in which division is always uniquely possible. *Trans. Amer. Math. Soc.*, 7(4):514–522, 1906.

[25] G. Ebert, G. Marino, O. Polverino, and R. Trombetti. On the multiplication of some semifields of order q^6. *Finite Fields Appl.*, 15(2):160–173, 2009.

[26] R. Gow and J. Sheekey. On primitive elements in finite semifields. *Finite Fields Appl.*, 17(2):194–204, 2011.

[27] Yutaka H. Automorphisms of p-groups of semifield type. *Osaka J. Math.*, 20(4):735–746, 1983.

[28] M. Hall. Projective planes. *Trans. Amer. Math. Soc.*, 54:229–277, 1943.

[29] D. R. Hughes and E. Kleinfeld. Seminuclear extensions of Galois fields. *Amer. J. Math.*, 82:389–392, 1960.

[30] D. R. Hughes and F. C. Piper. *Projective planes.* Springer-Verlag, New York, 1973. Graduate Texts in Mathematics, Vol. 6.

[31] V. Jha and N. L. Johnson. The dimension of a subplane of a translation plane. *Bull. Belg. Math. Soc. Simon Stevin*, 17(3):463–477, 2010.

[32] N L. Johnson, V. Jha, and M. Biliotti. *Handbook of finite translation planes*, volume 289 of *Pure and Applied Mathematics (Boca Raton)*. Chapman & Hall/CRC, Boca Raton, FL, 2007.

[33] N. L. Johnson, G. Marino, O. Polverino, and R. Trombetti. Semifields of order q^6 with left nucleus $\mathbb{F}_{q^3}$ and center $\mathbb{F}_q$. *Finite Fields Appl.*, 14(2):456–469, 2008.

[34] N. L. Johnson, G. Marino, O. Polverino, and R. Trombetti. On a generalization of cyclic semifields. *J. Algebraic Combin.*, 29(1):1–34, 2009.

[35] W. M. Kantor. Commutative semifields and symplectic spreads. *J. Algebra*, 270(1):96–114, 2003.

[36] W. M. Kantor. Finite semifields. In *Finite geometries, groups, and computation (Editors A. Hulpke, R. Liebler, T. Penttila, À Seres)*, pages 103–114. Walter de Gruyter GmbH & Co. KG, Berlin, 2006.

[37] W. M. Kantor. HMO-planes. *Adv. Geom.*, 9(1):31–43, 2009.

[38] W. M. Kantor and R. A. Liebler. Semifields arising from irreducible semilinear transformations. *J. Aust. Math. Soc.*, 85(3):333–339, 2008.

[39] I. Kaplansky. Infinite-dimensional quadratic forms admitting composition. *Proc. Amer. Math. Soc.*, 4:956–960, 1953.

[40] E. Kleinfeld. Techniques for enumerating Veblen-Wedderburn systems. *J. Assoc. Comput. Mach.*, 7:330–337, 1960.

[41] D. E. Knuth. Finite semifields and projective planes - phd. *PhD Dissertation*, pages 1–70, 1963.

[42] D. E. Knuth. Finite semifields and projective planes. *J. Algebra*, 2:182–217, 1965.

[43] M. Lavrauw. *Scattered spaces with respect to spreads, and eggs in finite projective spaces.* Eindhoven University of Technology, Eindhoven, 2001. Dissertation, Technische Universiteit Eindhoven, Eindhoven, 2001.

[44] M. Lavrauw. The two sets of three semifields associated with a semifield flock. *Innov. Incidence Geom.*, 2:101–107, 2005.

[45] M. Lavrauw. Sublines of prime order contained in the set of internal points of a conic. *Des. Codes Cryptogr.*, 38(1):113–123, 2006.

[46] M. Lavrauw. On the isotopism classes of finite semifields. *Finite Fields Appl.*, 14(4):897–910, 2008.

[47] M. Lavrauw. Finite semifields with a large nucleus and higher secant varieties to Segre varieties. *Adv. Geom.*, 11:399–410, 2011.

[48] M. Lavrauw and O. Polverino. Finite semifields and Galois geometry. *Chapter in Current research topics in Galois Geometry (Editors J. De Beule and L. Storme), NOVA Academic Publishers. ISBN 978-1-61209-523-3*, 2011.

[49] M. Lavrauw and J. Sheekey. Semifields from skew polynomial rings. *To appear in Adv. Geom.*

[50] M. Lavrauw and G. Van de Voorde. On linear sets on a projective line. *Des. Codes Cryptogr.*, 56(2-3):89–104, 2010.

[51] R. A. Liebler. Autotopism group representations. *J. London Math. Soc. (2)*, 23(1):85–91, 1981.

[52] R. A. Liebler. On nonsingular tensors and related projective planes. *Geom. Dedicata*, 11(4):455–464, 1981.

[53] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti. Translation dual of a semifield. *J. Combin. Theory Ser. A*, 115(8):1321–1332, 2008.

[54] G. Lunardon, G. Marino, O. Polverino, and R. Trombetti. Symplectic semifield spreads of $\mathrm{PG}(5, q)$ and the Veronese surface. *Ric. Mat.*, 60(1):125–142, 2011.

[55] D. M. Maduram. Transposed translation planes. *Proc. Amer. Math. Soc.*, 53(2):265–270, 1975.

[56] G. Marino and O. Polverino. On the nuclei of a finite semifield. *Preprint.*

[57] G. Marino, O. Polverino, and R. Trombetti. On $\mathbb{F}_q$-linear sets of $\mathrm{PG}(3, q^3)$ and semifields. *J. Combin. Theory Ser. A*, 114(5):769–788, 2007.

[58] G. Menichetti. On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field. *J. Algebra*, 47(2):400–410, 1977.

[59] G. Menichetti. n-dimensional algebras over a field with a cyclic extension of degree n. *Geom. Dedicata*, 63(1):69–94, 1996.

[60] G. P. Nagy. On the multiplication groups of semifields. *European J. Combin.*, 31(1):18–24, 2010.

[61] T. Penttila and B. Williams. Ovoids of parabolic spaces. *Geom. Dedicata*, 82(1-3):1–19, 2000.

[62] O. Polverino. Linear sets in finite projective spaces. *Discrete Math.*, 310(22):3096–3107, 2010.

[63] O. Polverino and R. Trombetti. Fractional dimension of binary knuth semifield planes. *J. Combin. Des.*, 20(7):317–327, 2012.

[64] A. Pott and Y. Zhou. A character theoretic approach to planar functions. *Cryptography and Communications*, 3:293–300, 2011.

[65] I. F. Rúa, E. F. Combarro, and J. Ranilla. Classification of semifields of order 64. *J. Algebra*, 322(11):4011–4029, 2009.

[66] I. F. Rúa, E. F. Combarro, and J. Ranilla. Computational methods for finite semifields. *Proceedings of the International Conference on Computational and Mathematical Methods in Science and Engineering, CMMCSE*, pages 937–1461, 2009.

[67] I. R. Rúa. Primitive and non primitive finite semifields. *Comm Algeb*, 32(2):793–803, 2004.

[68] L. A. Skornyakov. Alternative fields. *Ukrain. Mat. Žurnal*, 2:70–85, 1950.

[69] J. A. Thas. Generalized quadrangles of order (s, s^2). I. *J. Combin. Theory Ser. A*, 67(2):140–160, 1994.

[70] J. A. Thas. Generalized quadrangles of order (s, s^2). II. *J. Combin. Theory Ser. A*, 79(2):223–254, 1997.

[71] R. J. Walker. Determination of division algebras with 32 elements. In *Proc. Sympos. Appl. Math., Vol. XV*, pages 83–85. Amer. Math. Soc., Providence, R.I., 1963.

[72] M. Zorn. Theorie der alternativen ringe. *Abhandlungen aus dem Mathematischen Seminar der Universitt Hamburg*, 8:123–147, 1931.